UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,200,232 B2
APPLICATION NO. : 09/818567
DATED : April 3, 2007
INVENTOR(S) : S. Furuya et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Col. 25, lines 29-67 thru col. 26, lines 1 and 2; lines 23-64; and col. 27, beginning with line 22 thru col. 28, ending with line 23. Please amend claims 1, 5 and 10 as follows:

--1. (currently amended) A symmetric-key decryption method performed by a computer, comprising the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said ciphertext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (~~2 ≤i, i being~~ 2<=i<= a number indicative of ciphertext blocks) comprises:

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step. --

-- 5. (currently amended) A symmetric-key decryption apparatus comprising:

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

a circuit for dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

a random number generation circuit for generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

a decryption operation circuit for performing decryption operations to produce plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

a circuit for concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

a circuit for examining the redundancy data to detect whether the plaintext obtained from ciphertext has been altered,

wherein said decryption operation circuit for producing a plaintext block i corresponding to the ciphertext block i (~~2 ≤i, i being~~ 2<=i<= a number indicative of ciphertext blocks) comprises:

a first circuit for performing a first operation on said ciphertext block i,

a second circuit for performing a second operation on a result of said first operation performed on said ciphertext block i and said first random block corresponding to said ciphertext block i, and

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

a third circuit for performing a third operation on a result of said second operation performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce a result of said third operation as said plaintext block i, and

wherein said first circuit performs the first operation on said ciphertext block i and a result of said second operation performed on said ciphertext block i-1, and

wherein either said first random number or said second random number, which is generated by said random number generation circuit, is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation. --

-- 10. (currently amended) A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said program when executed causes said computer to perform the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (~~2 ≦i, i being~~2<=i<= a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i; and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,200,232 B2
APPLICATION NO. : 09/818567
DATED : April 3, 2007
INVENTOR(S) : S. Furuya et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step. --

Signed and Sealed this

Twenty-sixth Day of May, 2009

John Doll

JOHN DOLL
Acting Director of the United States Patent and Trademark Office